NIST SP 800-53: Empowered by OSCAL

National Institute of Standards and Technology
U.S. Department of Commerce

Victoria Yan Pillitteri
victoria.yan@nist.gov

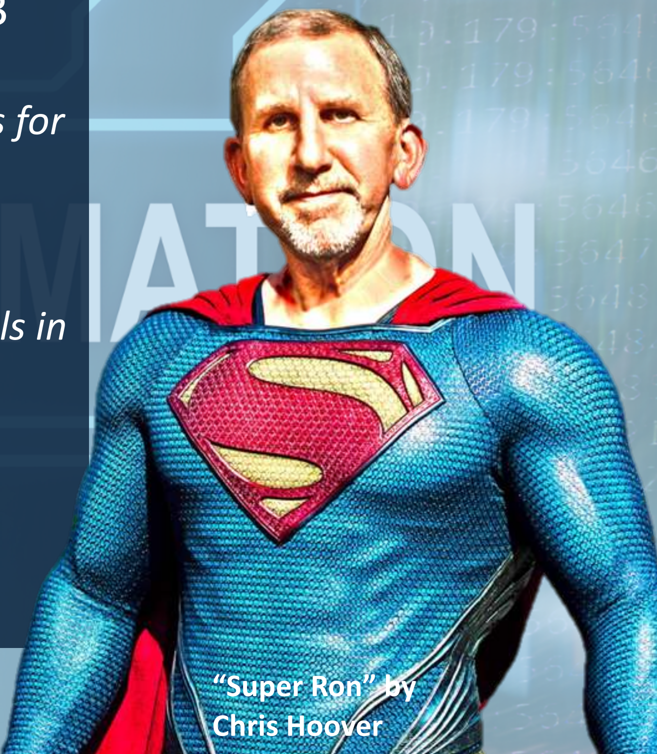
Agenda

✓ Development of the NIST Special Publication (SP) 800-53 suite before and after teaming with OSCAL

- SP 800-53 Revision (Rev) 5, *Security and Privacy Controls for Information Systems and Organizations*
- SP 800-53B, *Control Baselines for Information Systems and Organizations*
- SP 800-53A Rev 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*

✓ The Future of SP 800-53, Revision 6 and Beyond

✓ Q&A and Contact Information



“Super Ron” by Chris Hoover

NIST SP 800-53 at a glance

Security and Privacy Controls for Information Systems and Organizations

CATALOG OF **SECURITY & PRIVACY** CONTROLS

USED AS PART OF A **RISK MANAGEMENT** PROCESS

APPLICABLE TO **ALL TYPES** OF SYSTEMS & ORGANIZATIONS

6 REVISIONS SINCE **2005**

INTERNATIONAL USE AND IMPACT

AVAILABLE IN **MULTIPLE DATA FORMATS**

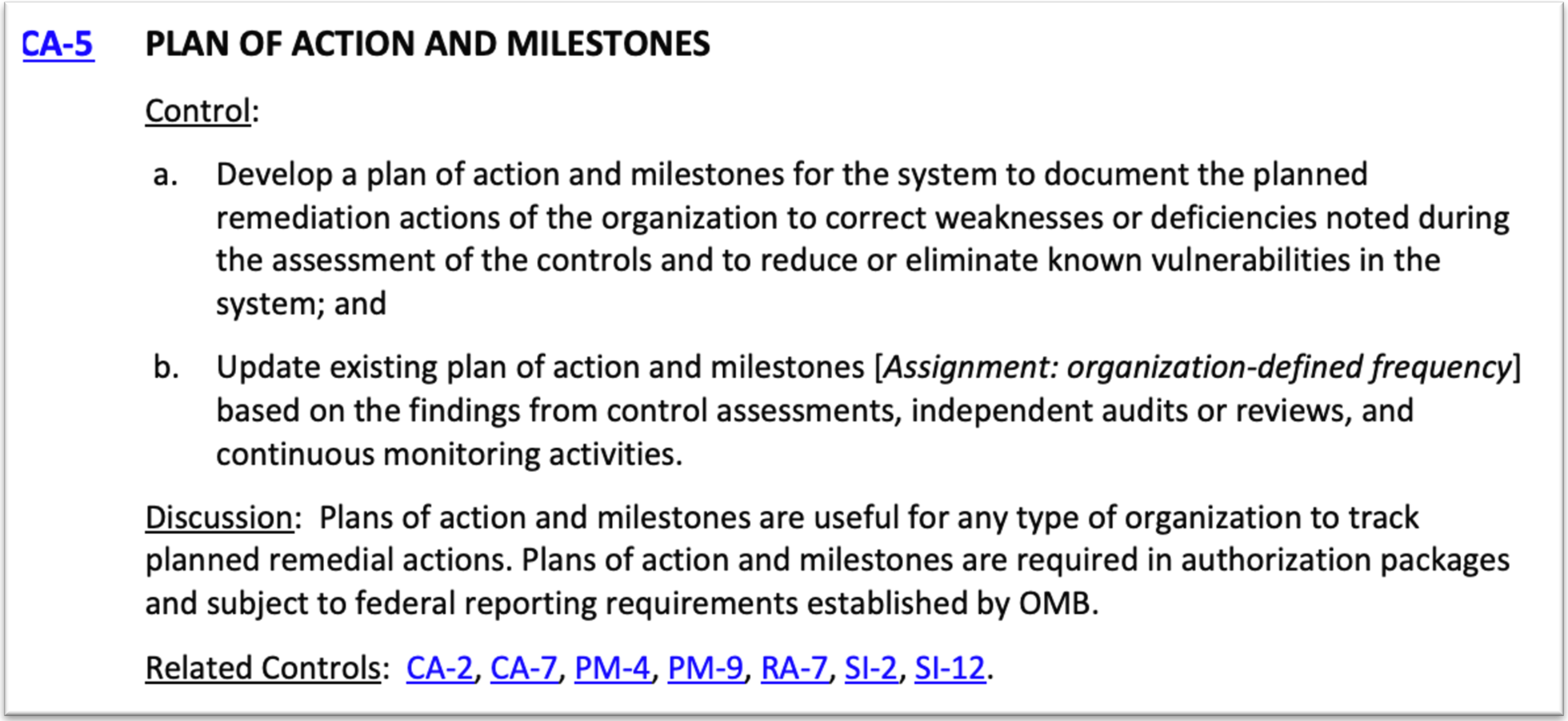
ASSESSMENT PROCEDURES **SP 800-53A**

CONTROL BASELINES **SP 800-53B**

SUBMIT YOUR **COMMENTS 24/7**

NIST SP 800-53 Rev 5

Security and Privacy Controls for Information Systems and Organizations



CA-5 **PLAN OF ACTION AND MILESTONES**

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

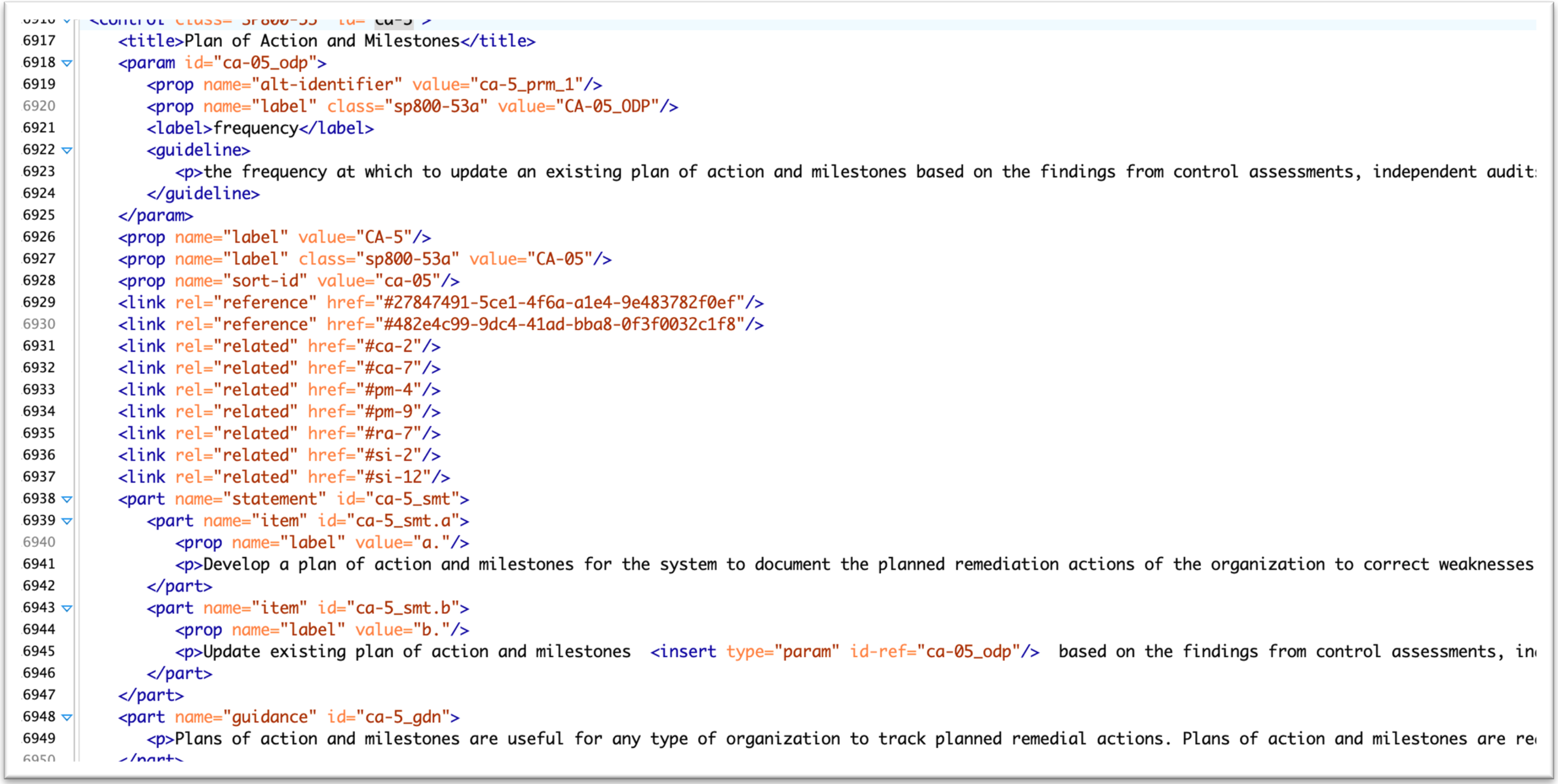
Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

STEP 1

DOC

NIST SP 800-53 Rev 5 in OSCAL



```
<control class="sp800-53" id="ca-5">
    <title>Plan of Action and Milestones</title>
    <param id="ca-05_odp">
       <prop name="alt-identifier" value="ca-5_prm_1"/>
       <prop name="label" class="sp800-53a" value="CA-05_ODP"/>
       <label>frequency</label>
       <guideline>
          <p>the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audit:
       </guideline>
    </param>
    <prop name="label" value="CA-5"/>
    <prop name="label" class="sp800-53a" value="CA-05"/>
    <prop name="sort-id" value="ca-05"/>
    <link rel="reference" href="#27847491-5ce1-4f6a-a1e4-9e483782f0ef"/>
    <link rel="reference" href="#482e4c99-9dc4-41ad-bba8-0f3f0032c1f8"/>
    <link rel="related" href="#ca-2"/>
    <link rel="related" href="#ca-7"/>
    <link rel="related" href="#pm-4"/>
    <link rel="related" href="#pm-9"/>
    <link rel="related" href="#ra-7"/>
    <link rel="related" href="#si-2"/>
    <link rel="related" href="#si-12"/>
    <part name="statement" id="ca-5_smt">
       <part name="item" id="ca-5_smt.a">
          <prop name="label" value="a."/>
          <p>Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses
       </part>
       <part name="item" id="ca-5_smt.b">
          <prop name="label" value="b."/>
          <p>Update existing plan of action and milestones  <insert type="param" id-ref="ca-05_odp"/>  based on the findings from control assessments, in
       </part>
    </part>
    <part name="guidance" id="ca-5_gdn">
       <p>Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are re
    </part>
```

STEP 2

NIST SP 800-53B

Control Baselines for Information Systems and Organizations

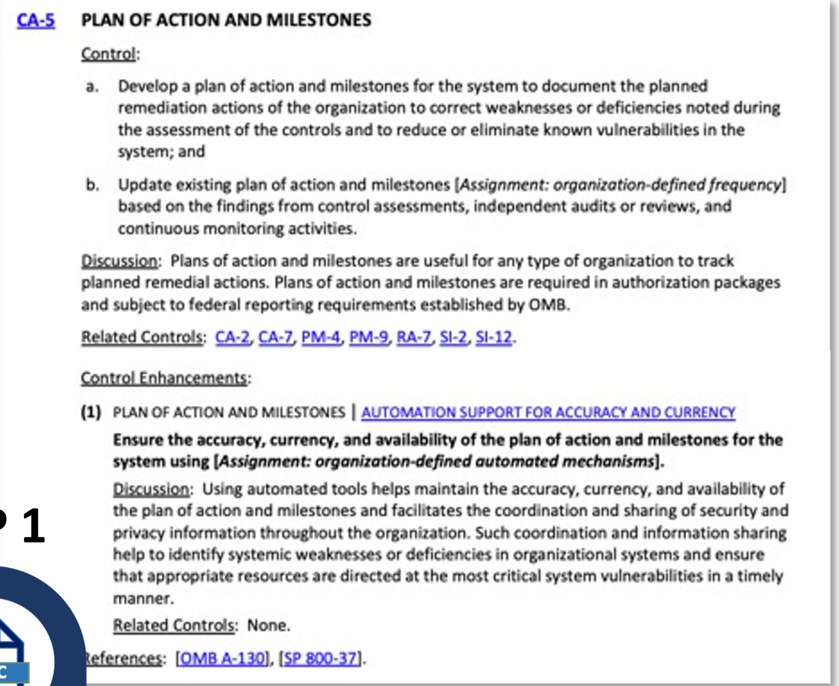
https://csrc.nist.gov/publications/detail/sp/800-53b/final

- ✓ **Three security control baselines** *(one for each system impact level – low-impact, moderate-impact, and high-impact)*

- ✓ **One privacy control baseline** *based on Federal Privacy Program Responsibilities per OMB Circular A-130*

- ✓ **Tailoring and overlay development guidance** to inform control selection process

NIST SP 800-53B in OSCAL



CA-5 **PLAN OF ACTION AND MILESTONES**

Control:

a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Discussion: Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of action and milestones are required in authorization packages and subject to federal reporting requirements established by OMB.

Related Controls: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Control Enhancements:

(1) PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY

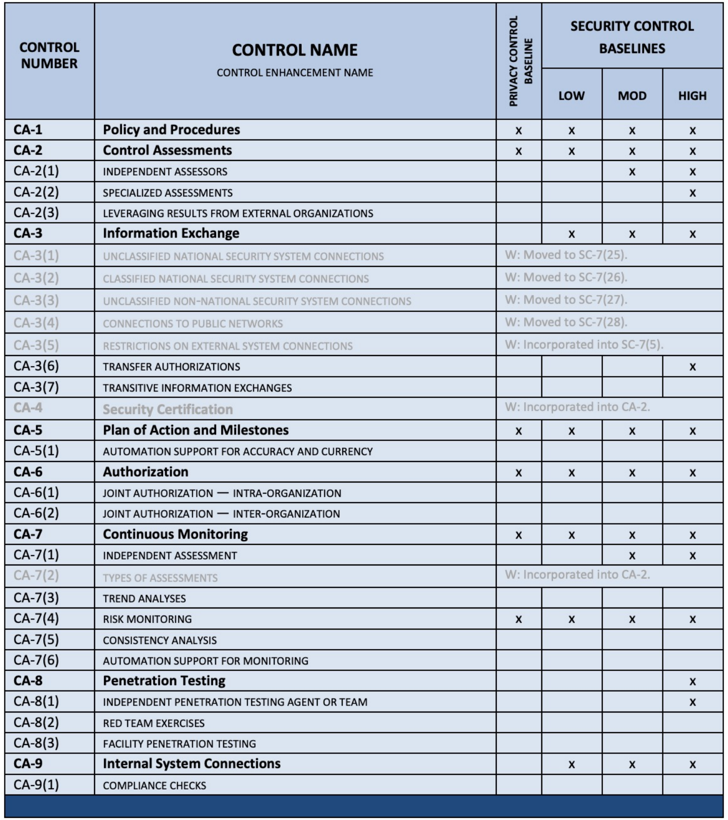
Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [*Assignment: organization-defined automated mechanisms*].

Discussion: Using automated tools helps maintain the accuracy, currency, and availability of the plan of action and milestones and facilitates the coordination and sharing of security and privacy information throughout the organization. Such coordination and information sharing help to identify systemic weaknesses or deficiencies in organizational systems and ensure that appropriate resources are directed at the most critical system vulnerabilities in a timely manner.

Related Controls: None.

References: [OMB A-130], [SP 800-37].

NIST SP 800-53 Revision 5 and NIST SP 800-53B

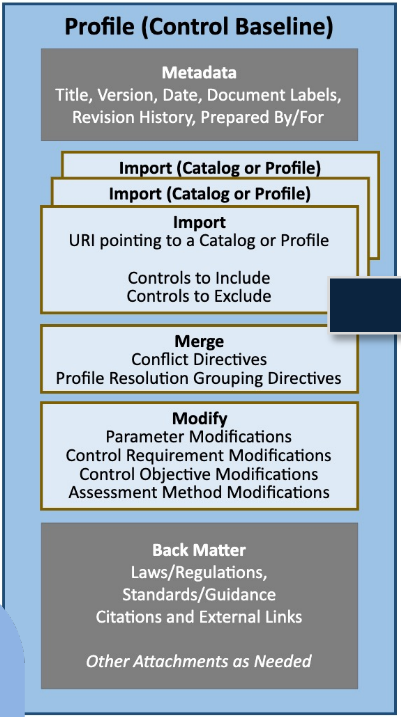


CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
CA-1	**Policy and Procedures**	x	x	x	x
CA-2	**Control Assessments**	x	x	x	x
CA-2(1)	INDEPENDENT ASSESSORS			x	x
CA-2(2)	SPECIALIZED ASSESSMENTS				x
CA-2(3)	LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS				
CA-3	**Information Exchange**		x	x	x
CA-3(1)	UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(25).			
CA-3(2)	CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(26).			
CA-3(3)	UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	W: Moved to SC-7(27).			
CA-3(4)	CONNECTIONS TO PUBLIC NETWORKS	W: Moved to SC-7(28).			
CA-3(5)	RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS	W: Incorporated into SC-7(5).			
CA-3(6)	TRANSFER AUTHORIZATIONS				x
CA-3(7)	TRANSITIVE INFORMATION EXCHANGES				
CA-4	Security Certification	W: Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**	x	x	x	x
CA-5(1)	AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY				
CA-6	**Authorization**	x	x	x	x
CA-6(1)	JOINT AUTHORIZATION — INTRA-ORGANIZATION				
CA-6(2)	JOINT AUTHORIZATION — INTER-ORGANIZATION				
CA-7	**Continuous Monitoring**	x	x	x	x
CA-7(1)	INDEPENDENT ASSESSMENT			x	x
CA-7(2)	TYPES OF ASSESSMENTS	W: Incorporated into CA-2.			
CA-7(3)	TREND ANALYSES				
CA-7(4)	RISK MONITORING	x	x	x	x
CA-7(5)	CONSISTENCY ANALYSIS				
CA-7(6)	AUTOMATION SUPPORT FOR MONITORING				
CA-8	**Penetration Testing**				x
CA-8(1)	INDEPENDENT PENETRATION TESTING AGENT OR TEAM				x
CA-8(2)	RED TEAM EXERCISES				
CA-8(3)	FACILITY PENETRATION TESTING				
CA-9	**Internal System Connections**		x	x	x
CA-9(1)	COMPLIANCE CHECKS				

STEP 1

DOC

NIST SP 800-53B in OSCAL



Profile (Control Baseline)

Metadata
Title, Version, Date, Document Labels, Revision History, Prepared By/For

Import (Catalog or Profile)

Import (Catalog or Profile)

Import
URI pointing to a Catalog or Profile

Controls to Include
Controls to Exclude

Merge
Conflict Directives
Profile Resolution Grouping Directives

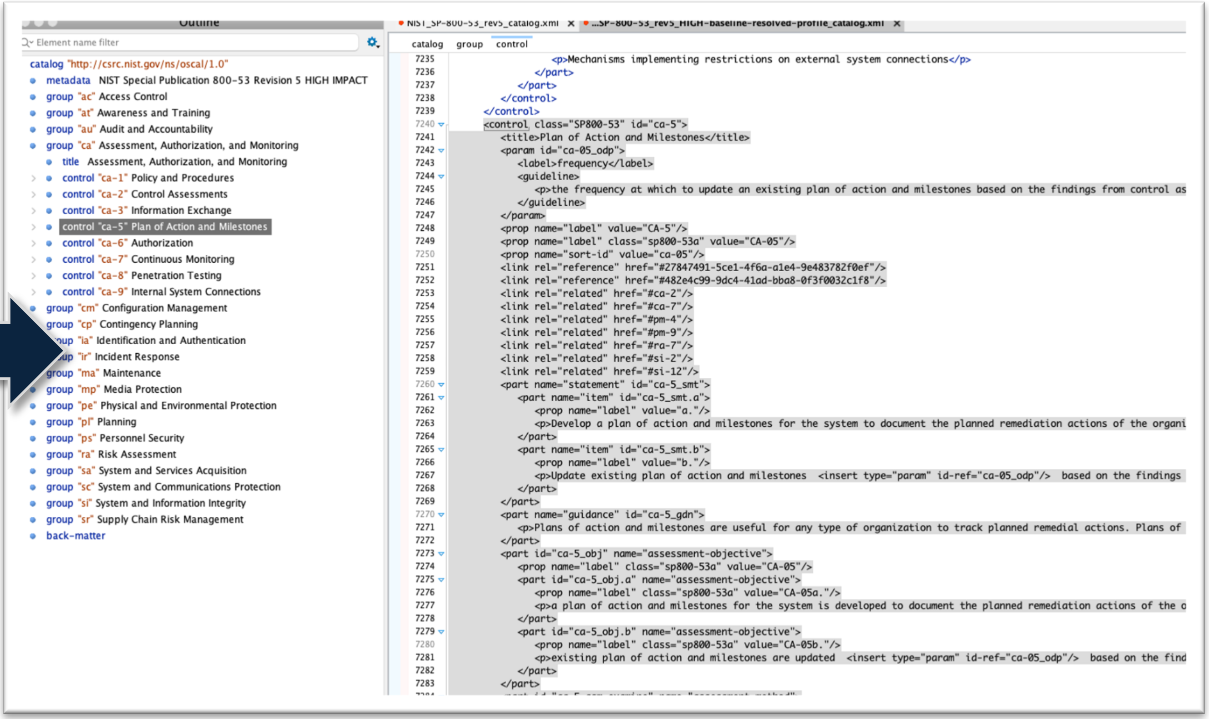
Modify
Parameter Modifications
Control Requirement Modifications
Control Objective Modifications
Assessment Method Modifications

Back Matter
Laws/Regulations, Standards/Guidance
Citations and External Links

Other Attachments as Needed

OSCAL Profile Model

STEP 2



Outline
Element name filter
NIST_SP-800-53_rev5_catalog.xml
...SP-800-53_rev5_HIGH-baseline-resolved-profile_catalog.xml
catalog
group
control

- catalog "http://csrc.nist.gov/ns/oscal/1.0"
  - metadata NIST Special Publication 800-53 Revision 5 HIGH IMPACT
  - group "ac" Access Control
  - group "at" Awareness and Training
  - group "au" Audit and Accountability
  - group "ca" Assessment, Authorization, and Monitoring
    - title Assessment, Authorization, and Monitoring
    - control "ca-1" Policy and Procedures
    - control "ca-2" Control Assessments
    - control "ca-3" Information Exchange
    - control "ca-5" Plan of Action and Milestones
    - control "ca-6" Authorization
    - control "ca-7" Continuous Monitoring
    - control "ca-8" Penetration Testing
    - control "ca-9" Internal System Connections
  - group "cm" Configuration Management
  - group "cp" Contingency Planning
  - group "ia" Identification and Authentication
  - group "ir" Incident Response
  - group "ma" Maintenance
  - group "mp" Media Protection
  - group "pe" Physical and Environmental Protection
  - group "pl" Planning
  - group "ps" Personnel Security
  - group "ra" Risk Assessment
  - group "sa" System and Services Acquisition
  - group "sc" System and Communications Protection
  - group "si" System and Information Integrity
  - group "sr" Supply Chain Risk Management
  - back-matter

```xml
        <p>Mechanisms implementing restrictions on external system connections</p>
      </part>
    </part>
  </control>
</control>
<control class="SP800-53" id="ca-5">
  <title>Plan of Action and Milestones</title>
  <param id="ca-05_odp">
    <label>frequency</label>
    <guideline>
      <p>the frequency at which to update an existing plan of action and milestones based on the findings from control as
    </guideline>
  </param>
  <prop name="label" value="CA-5"/>
  <prop name="label" class="sp800-53a" value="CA-05"/>
  <prop name="sort-id" value="ca-05"/>
  <link rel="reference" href="#27847491-5ce1-4f6a-a1e4-9e483782f0ef"/>
  <link rel="reference" href="#482e4c99-9dc4-41ad-bba8-0f3f0032c1f8"/>
  <link rel="related" href="#ca-2"/>
  <link rel="related" href="#ca-7"/>
  <link rel="related" href="#pm-4"/>
  <link rel="related" href="#pm-9"/>
  <link rel="related" href="#ra-7"/>
  <link rel="related" href="#si-2"/>
  <link rel="related" href="#si-12"/>
  <part name="statement" id="ca-5_smt">
    <part name="item" id="ca-5_smt.a">
      <prop name="label" value="a."/>
      <p>Develop a plan of action and milestones for the system to document the planned remediation actions of the organi
    </part>
    <part name="item" id="ca-5_smt.b">
      <prop name="label" value="b."/>
      <p>Update existing plan of action and milestones  <insert type="param" id-ref="ca-05_odp"/>  based on the findings
    </part>
  </part>
  <part name="guidance" id="ca-5_gdn">
    <p>Plans of action and milestones are useful for any type of organization to track planned remedial actions. Plans of
  </part>
  <part id="ca-5_obj" name="assessment-objective">
    <prop name="label" class="sp800-53a" value="CA-05"/>
    <part id="ca-5_obj.a" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05a."/>
      <p>a plan of action and milestones for the system is developed to document the planned remediation actions of the o
    </part>
    <part id="ca-5_obj.b" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05b."/>
      <p>existing plan of action and milestones are updated  <insert type="param" id-ref="ca-05_odp"/>  based on the find
    </part>
  </part>
```

SP 800-53 Baseline Profiles

SP 800-53 Rev 5 HIGH Baseline Shown

NIST SP 800-53A Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

To facilitate (SP 800-53) control assessments within an effective risk management framework

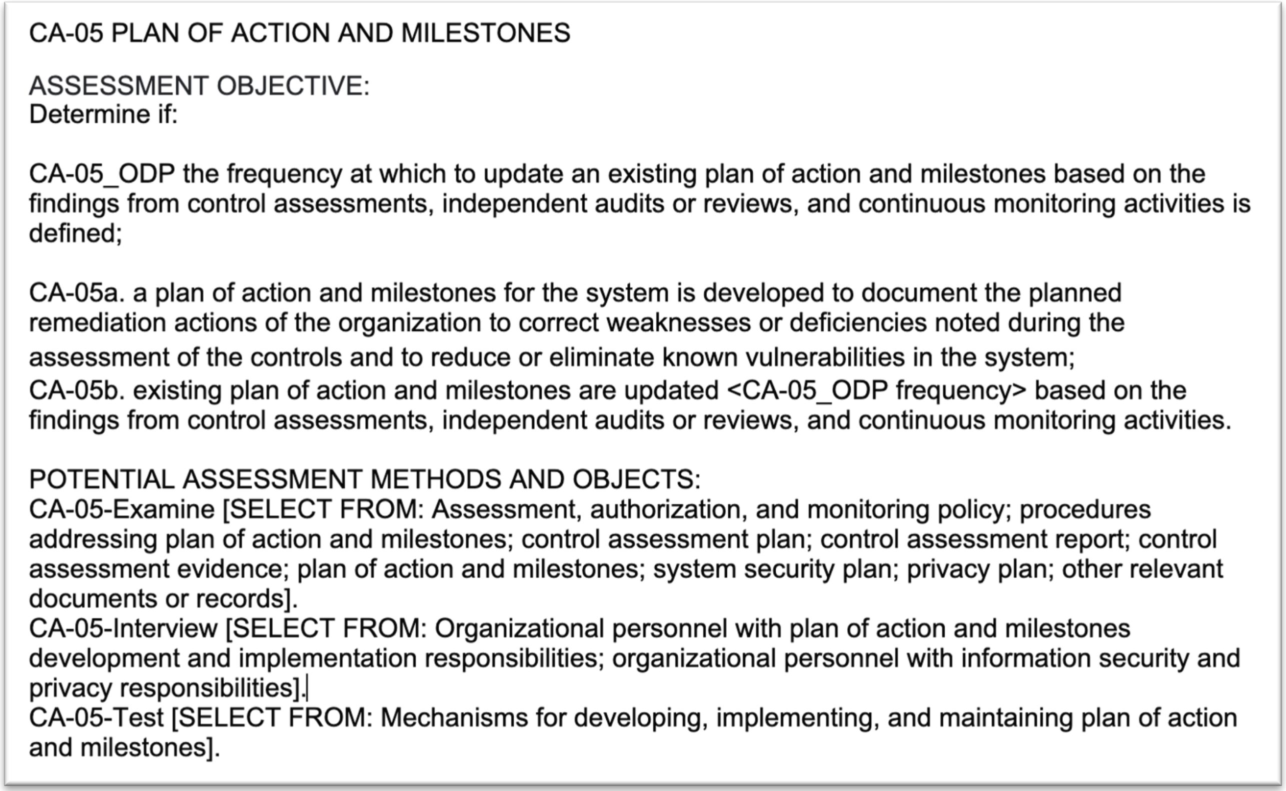
1. Process to conduct effective control assessments (Prepare, Develop Plans, Conduct Assessments, Analyze Results)
2. (Initial) assessment procedures that correspond with SP 800-53 Rev 5 controls

SP 800-53 control assessments:

✓ Determine overall effectiveness of implemented controls	🚫 Checklist for compliance
✓ Indication of quality of risk management process	🚫 Simple pass/fail results
✓ Information about security & privacy strengths/weaknesses of the system/organization	🚫 Paperwork exercise to pass inspections/audits

https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

Developing NIST SP 800-53A Rev 5



CA-05 PLAN OF ACTION AND MILESTONES

ASSESSMENT OBJECTIVE:
Determine if:

CA-05_ODP the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities is defined;

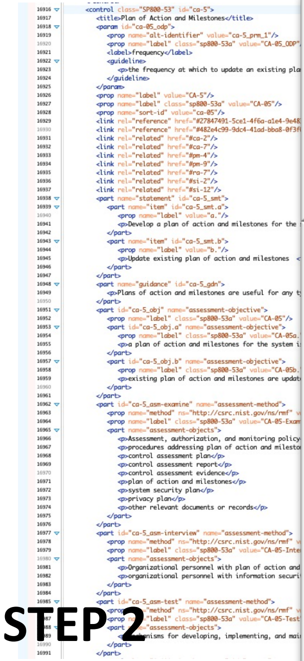
CA-05a. a plan of action and milestones for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;
CA-05b. existing plan of action and milestones are updated <CA-05_ODP frequency> based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

POTENTIAL ASSESSMENT METHODS AND OBJECTS:
CA-05-Examine [SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing plan of action and milestones; control assessment plan; control assessment report; control assessment evidence; plan of action and milestones; system security plan; privacy plan; other relevant documents or records].
CA-05-Interview [SELECT FROM: Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security and privacy responsibilities].
CA-05-Test [SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action and milestones].

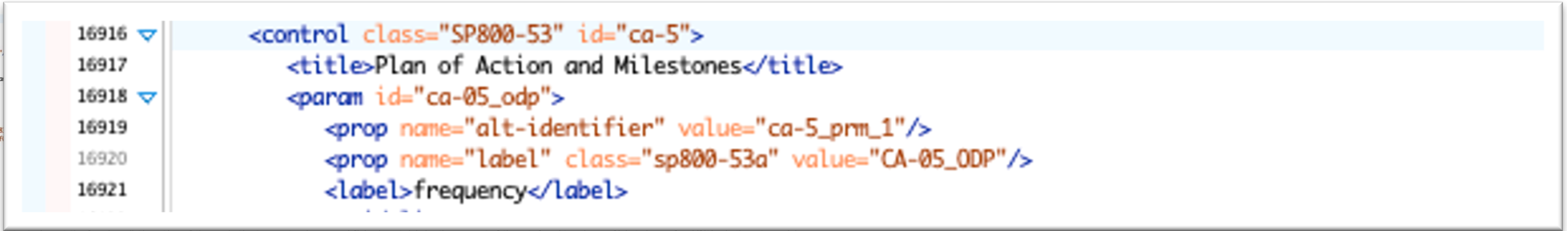
STEP 1

TXT

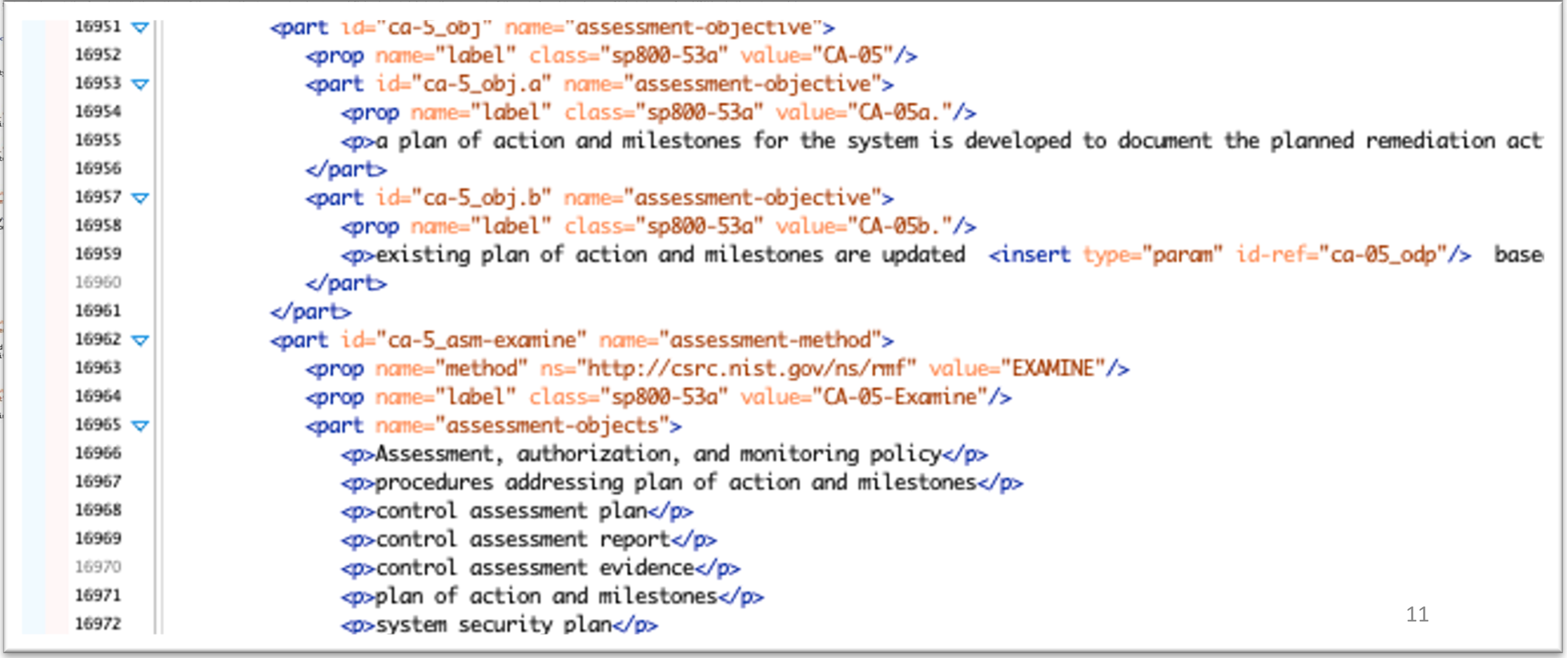
SP 800-53A Rev 5 in OSCAL



```xml
<control class="SP800-53" id="ca-5">
   <title>Plan of Action and Milestones</title>
   <param id="ca-05_odp">
      <prop name="alt-identifier" value="ca-5_prm_1"/>
      <prop name="label" class="sp800-53a" value="CA-05_ODP"
      <label>frequency</label>
      <guideline>
         <p>the frequency at which to update an existing pla
      </guideline>
   </param>
   <prop name="label" value="CA-5"/>
   <prop name="label" class="sp800-53a" value="CA-05"/>
   <prop name="sort-id" value="ca-05"/>
   <link rel="reference" href="#27847491-5ce1-4f6a-a1e4-9e48
   <link rel="reference" href="#482e4c99-9dc4-41ad-bba8-0f3f
   <link rel="related" href="#ca-2"/>
   <link rel="related" href="#ca-7"/>
   <link rel="related" href="#pm-4"/>
   <link rel="related" href="#pm-9"/>
   <link rel="related" href="#ra-7"/>
   <link rel="related" href="#si-2"/>
   <link rel="related" href="#si-12"/>
   <part name="statement" id="ca-5_smt">
      <part name="item" id="ca-5_smt.a">
         <prop name="label" value="a."/>
         <p>Develop a plan of action and milestones for the
      </part>
      <part name="item" id="ca-5_smt.b">
         <prop name="label" value="b."/>
         <p>Update existing plan of action and milestones  <
      </part>
   </part>
   <part name="guidance" id="ca-5_gdn">
      <p>Plans of action and milestones are useful for any t
   </part>
   <part id="ca-5_obj" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05"/>
      <part id="ca-5_obj.a" name="assessment-objective">
         <prop name="label" class="sp800-53a" value="CA-05a.
         <p>a plan of action and milestones for the system i
      </part>
      <part id="ca-5_obj.b" name="assessment-objective">
         <prop name="label" class="sp800-53a" value="CA-05b.
         <p>existing plan of action and milestones are updat
      </part>
   </part>
   <part id="ca-5_asm-examine" name="assessment-method">
      <prop name="method" ns="http://csrc.nist.gov/ns/rmf" v
      <prop name="label" class="sp800-53a" value="CA-05-Exam
      <part name="assessment-objects">
         <p>Assessment, authorization, and monitoring policy
         <p>procedures addressing plan of action and milesto
         <p>control assessment plan</p>
         <p>control assessment report</p>
         <p>control assessment evidence</p>
         <p>plan of action and milestones</p>
         <p>system security plan</p>
         <p>privacy plan</p>
         <p>other relevant documents or records</p>
      </part>
   </part>
   <part id="ca-5_asm-interview" name="assessment-method">
      <prop name="method" ns="http://csrc.nist.gov/ns/rmf" v
      <prop name="label" class="sp800-53a" value="CA-05-Inte
      <part name="assessment-objects">
         <p>Organizational personnel with plan of action and
         <p>organizational personnel with information securi
      </part>
   </part>
   <part id="ca-5_asm-test" name="assessment-method">
      <prop name="method" ns="http://csrc.nist.gov/ns/rmf" v
      <prop name="label" class="sp800-53a" value="CA-05-Test
      <part name="assessment-objects">
         <p>mechanisms for developing, implementing, and mai
      </part>
   </part>
```



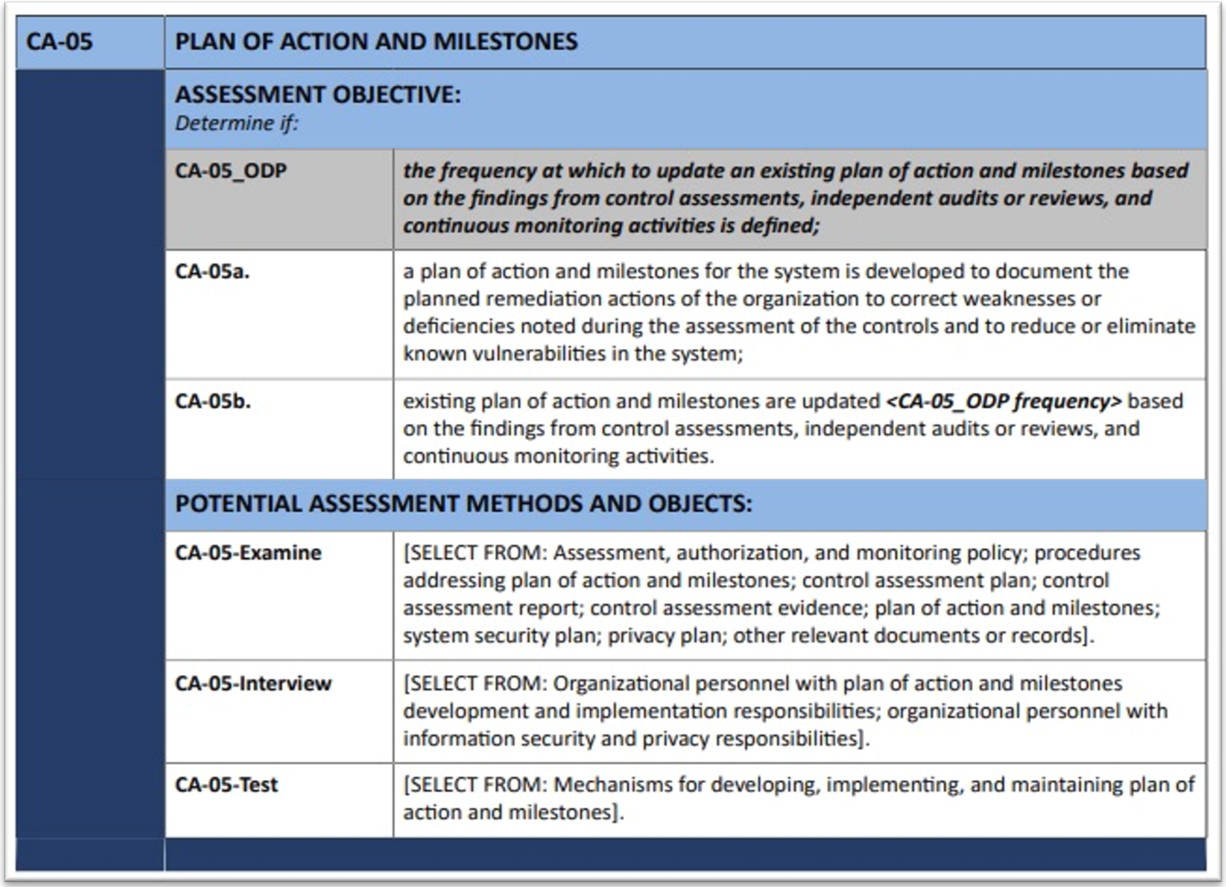
```xml
<control class="SP800-53" id="ca-5">
   <title>Plan of Action and Milestones</title>
   <param id="ca-05_odp">
      <prop name="alt-identifier" value="ca-5_prm_1"/>
      <prop name="label" class="sp800-53a" value="CA-05_ODP"/>
      <label>frequency</label>
```



```xml
<part id="ca-5_obj" name="assessment-objective">
   <prop name="label" class="sp800-53a" value="CA-05"/>
   <part id="ca-5_obj.a" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05a."/>
      <p>a plan of action and milestones for the system is developed to document the planned remediation act
   </part>
   <part id="ca-5_obj.b" name="assessment-objective">
      <prop name="label" class="sp800-53a" value="CA-05b."/>
      <p>existing plan of action and milestones are updated  <insert type="param" id-ref="ca-05_odp"/>  base
   </part>
</part>
<part id="ca-5_asm-examine" name="assessment-method">
   <prop name="method" ns="http://csrc.nist.gov/ns/rmf" value="EXAMINE"/>
   <prop name="label" class="sp800-53a" value="CA-05-Examine"/>
   <part name="assessment-objects">
      <p>Assessment, authorization, and monitoring policy</p>
      <p>procedures addressing plan of action and milestones</p>
      <p>control assessment plan</p>
      <p>control assessment report</p>
      <p>control assessment evidence</p>
      <p>plan of action and milestones</p>
      <p>system security plan</p>
```

STEP 2

Using OSCAL to create the SP 800-53A PDF



CA-05	PLAN OF ACTION AND MILESTONES
	ASSESSMENT OBJECTIVE: *Determine if:*
CA-05_ODP	***the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities is defined;***
CA-05a.	a plan of action and milestones for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;
CA-05b.	existing plan of action and milestones are updated ***<CA-05_ODP frequency>*** based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
CA-05-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing plan of action and milestones; control assessment plan; control assessment report; control assessment evidence; plan of action and milestones; system security plan; privacy plan; other relevant documents or records].
CA-05-Interview	[SELECT FROM: Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security and privacy responsibilities].
CA-05-Test	[SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action and milestones].

STEP 3

The Future of NIST SP 800-53

SP 800-53 Comment Site Available Today!

✓ Submit your comments & ideas on SP 800-53/53B

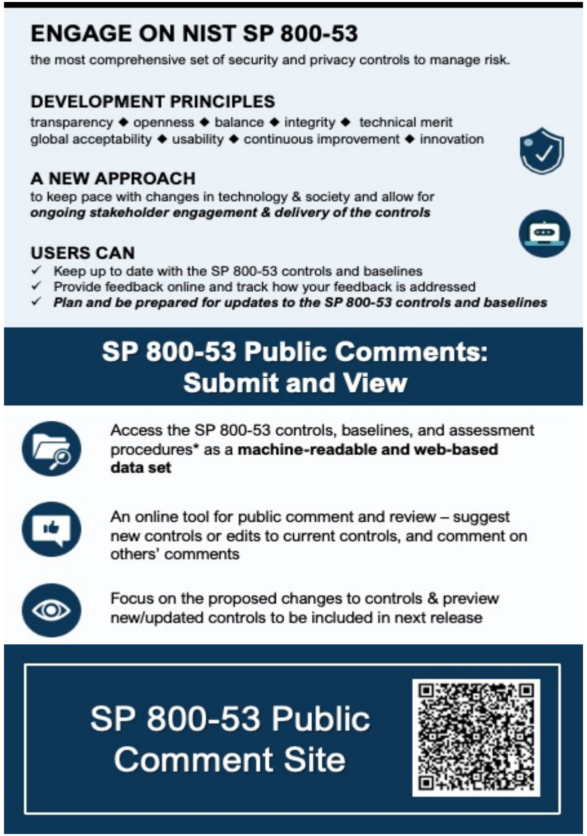
https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/public-comments

The NIST RMF Team is already planning for Revision 6

✓ **No planned date for Revision 6 yet**

✓ *For Revision 6*, NIST will release **controls, control baselines,** and **control assessment procedures concurrently** *(draft and final)* through the SP 800-53 Comment Site

SIMPLIFY | INNOVATE | AUTOMATE



ENGAGE ON NIST SP 800-53

the most comprehensive set of security and privacy controls to manage risk.

DEVELOPMENT PRINCIPLES

transparency ◆ openness ◆ balance ◆ integrity ◆ technical merit
global acceptability ◆ usability ◆ continuous improvement ◆ innovation

A NEW APPROACH

to keep pace with changes in technology & society and allow for
ongoing stakeholder engagement & delivery of the controls

USERS CAN

- ✓ Keep up to date with the SP 800-53 controls and baselines
- ✓ Provide feedback online and track how your feedback is addressed
- ✓ ***Plan and be prepared for updates to the SP 800-53 controls and baselines***

SP 800-53 Public Comments: Submit and View

Access the SP 800-53 controls, baselines, and assessment procedures* as a **machine-readable and web-based data set**

An online tool for public comment and review – suggest new controls or edits to current controls, and comment on others' comments

Focus on the proposed changes to controls & preview new/updated controls to be included in next release

SP 800-53 Public Comment Site

STAY IN TOUCH

CONTACT US

nist.gov/RMF

sec-cert@nist.gov

@NISTcyber